

Claims

What is claimed is:

- [c1] A method for conveying a security context, comprising:
creating and assigning a virtual address to a client process;
issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context;
prepending an issued packet with a second Internet Protocol version header
producing a second Internet Protocol version compliant packet;
forwarding the second Internet Protocol version compliant packet to a recipient;
stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient;
decrypting and authenticating the stripped packet using a particular method as indicated by the security context producing a decrypted and authenticated packet; and
routing the decrypted and authenticated packet to a recipient process using the virtual address.
- [c2] The method of claim 1, wherein the first Internet Protocol version compliant packet is Internet Protocol version 6 compliant packet.
- [c3] The method of claim 1, wherein the second Internet Protocol version compliant packet is Internet Protocol version 4 compliant packet.
- [c4] The method of claim 1, wherein issuing the packet further comprises:
executing a Supernet Attach Command with an authentication server daemon;
responding to the Supernet Attach Command with a Supernet configuration information comprising the security context in the address; and

registering a mapping of the Supernet configuration information with a virtual address daemon.

- [c5] The method of claim 1, wherein the security context in the address comprises the virtual address, a Supernet identity, and a channel identity.
- [c6] The method of claim 5, wherein the security context comprises a 128 bit unique value.
- [c7] The method of claim 6, wherein the security context comprises a 16 bit set and a 112 bit set.
- [c8] The method of claim 7, wherein the 16 bit set denotes a site local Internet protocol address comprising 12 bits for an address prefix followed by 4 bits for a zero value.
- [c9] The method of claim 7, wherein the 112 bit set comprises contiguous bits for the Supernet identifier, the Channel identifier, and the virtual address.
- [c10] The method of claim 7, wherein the 112 bit set comprises a 64 bit Supernet identifier, a 24 bit Channel identifier, and a 24 bit virtual address.
- [c11] The method of claim 4, wherein the virtual address daemon maps the virtual address of the recipient process within the Supernet to an actual Internet protocol address.
- [c12] The method of claim 1, wherein the security context is encoded.
- [c13] The method of claim 1, wherein the security context is obtained from the stripped packet using a handler mechanism.
- [c14] The method of claim 13, wherein the handler mechanism is a Netfilter.

[c15] A network system comprising:

an authentication server daemon that replies to a Supernet Attach Command; and
a virtual address daemon that maintains a mapping of the Supernet configuration information performing the following steps:
creating and assigning a virtual address to a client process;
issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context;
prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet;
forwarding the second Internet Protocol version compliant packet to a recipient;
stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient;
decrypting and authenticating the stripped packet using a particular method as indicated by the security context producing a decrypted and authenticated packet; and
routing the decrypted and authenticated packet to a recipient process using the virtual address.

[c16] The method of claim 15, wherein the first Internet Protocol version compliant packet is Internet Protocol version 6 compliant packet.

[c17] The method of claim 15, wherein the second Internet Protocol version compliant packet is Internet Protocol version 4 compliant packet.

[c18] The network system of claim 15, wherein issuing the packet further comprises:
executing a Supernet Attach Command with an authentication server daemon;
responding to the Supernet Attach Command with a Supernet configuration
information comprising the security context in the address; and

registering a mapping of the Supernet configuration information with a virtual address daemon.

- [c19] The network system of claim 18, wherein the security context in the address comprises the virtual address, a Supernet identity, and a Channel identity.
- [c20] The network system of claim 19, wherein the security context comprises a 128 bit unique value.
- [c21] The method of claim 20, wherein the security context comprises a 16 bit set and a 112 bit set.
- [c22] The method of claim 21, wherein the 16 bit set denotes a site local Internet protocol address comprising 12 bits for an address prefix followed by 4 bits for a zero value.
- [c23] The method of claim 21, wherein the 112 bit set comprises contiguous bits for the Supernet identifier, the Channel identifier, and the virtual address.
- [c24] The method of claim 21, wherein the 112 bit set comprises a 64 bit Supernet identifier, a 24 bit Channel identifier, and a 24 bit virtual address.
- [c25] The method of claim 18, wherein the virtual address daemon maps the virtual address of the recipient process within the Supernet to an actual Internet protocol address.
- [c26] The method of claim 15, wherein the security context is encoded.
- [c27] The method of claim 15, wherein the security context is obtained from the stripped packet using a handler mechanism.
- [c28] The method of claim 27, wherein the handler mechanism is a Netfilter.

- [c29] An apparatus for conveying a security context, comprising:
- means for creating and assigning a virtual address to a client process;
 - means for issuing a first Internet Protocol version compliant packet, wherein the first Internet Protocol version compliant packet comprises a security context;
 - means for prepending an issued packet with a second Internet Protocol version header producing a second Internet Protocol version compliant packet;
 - means for forwarding the second Internet Protocol version compliant packet to a recipient;
 - means for stripping away the second Internet Protocol version compliant header from the second Internet Protocol version compliant packet producing a stripped packet at the recipient;
 - means for decrypting and authenticating the stripped packet using a particular method as indicated by the security context producing a decrypted and authenticated packet; and
 - means for routing the decrypted and authenticated packet to a recipient process using the virtual address.